BEFORE THE

FEDERAL ENERGY REGULATORY COMMISSION

- - - - - - - - - - - - - - - - - - - -x

IN THE MATTER OF: :

REMEDYING UNDUE DISCRIMINATION THROUGH : Docket Number

OPEN ACCESS TRANSMISSION SERVICE AND : RM01-12-000

STANDARD ELECTRICITY MARKET DESIGN :

- - - - - - - - - - - - - - - - - - - -x

Commission Meeting Room

Federal Energy Regulatory

Commission

888 First Street, N.E.

Washington, D.C.

Tuesday, February 4, 2003

The above-entitled matter came on for conference, pursuant to notice, at 9:30 a.m., Alison Silverstein, presiding.

APPEARANCES:

ALISON SILVERSTEIN

CHUCK NOBLE

KEVIN PERRY

JONATHAN FIRST

LYNN CONSTANTINI

LOU LEFFLER

DAVE HILT

P R O C E E D I N G S

(9:30 a.m.)

MS. SILVERSTEIN: Okay, Roger, it's not a CIPAG meeting. Time to sit down.

Good morning, I'm Alison Silverstein. This is the Federal Energy Regulatory Commission and our third workshop on cyber security for the electric industry. I'd like to tell you what we're going to do in terms of today's program, but first I'm actually going to. When you say I'd like to, you sound like one of those people on the airplane who says, I'd like to do it, and then you wonder if they're actually going to deliver on it.

But let's start with the Pledge of Allegiance and a moment of silence please.

(Pledge recited, moment of silence observed.)

MS. SILVERSTEIN: Most of you have given us comments on the topics. We have, since the FERC started talking to the folks in the NERC security community back in April, we have discussed elements of the topics that are the subject of today's workshop. And many of you have addressed these in your comments that were filed in November? October? The comment schedule blurs. I apologize. But many of you have addressed these in your comments.

However, it seemed appropriate for us, since we have had an extensive discussion on the contents of the

security standards that are proposed themselves, it is time to discuss some of the issues that surround those standards and how FERC should implement them and when and so on and so forth. So we thought it was probably worthwhile to have that discussion here rather than within the context of the NERC Critical Infrastructure Protection Advisory Group because there is not a full participation of the community of interest in the NERC CIPAG to the degree that there is other FERC sponsored deal.

So here we are and my proposal for today is as follows. We're going to start with a presentation by David Hilt of the NERC on NERC's current and evolving compliance process, and that'll take us into the discussion of compliance that is the first set of issues to be discussed and will lead us into many of the other issues.

And one of the things I know many of you in the room, I know that you're not shy and my expectation is that some of you have points and you will want to participate aggressively in this discussion. So what I'm going to ask you to do is, after Dave's presentation -- let's see a show of hands right now of people who think that they're likely to want to leap out of their seats and talk.

(No response.)

MS. SILVERSTEIN: Okay, let's see a show of hands of the people who know that you're here only as a lurker to

make sure we don't do anything that you're not aware of.

(No response.)

MS. SILVERSTEIN: Okay. I guess this concludes our -- you don't even want to bother talking? No one actually wants to say anything, so we've all wasted our trips. Okay, Dave's going to give his presentation and then afterward, and we'll give you all the 20 minutes of his presentation to think about the following. Would you like to walk up and take one of these chairs with a microphone so we can actually have a discussion that doesn't involve you sitting at a seat waiving your hands, because I think these are the kind of issues that lend themselves more conveniently to a discussion among people who are facing each other than people who are just sitting in their seats trying to ignore each other. So that will be my goal and I hope that some of you share it, and will becoming up to the table. We have blank name tags so that we can identify you for our Court Reporter and we won't even make you commit yourself by picking up a blank name tag yet. You can do that after Dave's presentation.

And with me is Jonathan First who is a FERC attorney. So Dave, why don't you take it a way.

MR. HILT: There we go. Thank you. What I was asked to do, and I've not been deeply involved in the critical infrastructure protection activities that you folks

have been working with and that the CIPAG group has been working with.

What I was asked to do was come and talk a little bit about where we are and what's going on with the NERC Compliance Enforcement program and where we are. I am the Director of that program at NERC, have been there since 1999 when we really initiated the program, and we've been bringing the program up to speed ever since.

Some of the background that brings us here today, as I understand it, certainly in the FERC standard market design NOPR there's a proposal in one of the appendices. It talks about proposing cyber security standards and mandatory compliance with those standards via some self-certification mechanism.

When it came to compliance monitoring, I understand the issue came up at the last conference, how do we deal with compliance, and I think that was the purpose that Alison had stated here today is one of the topics to be covered, and there were some individuals that suggested that the FERC should look at NERC's Compliance Enforcement program as a potential vehicle. And certainly if we do have a program, that could be a potential tool here.

Just a little bit about the program. We really address four areas within the NERC program today. We do monitoring assessment and review to the NERC standards which

today are operating policies and planning standards. In the future, they will be reliability standards, new process and new standards under development based on much of that work that's underway today.

We also are involved with certification activities. Today we are doing personnel certification for system operators. We have an operator certification program where people are, by exam, certified as system operators, recognizing that they understand and pass certain requirements that they understand and can operate the system in accordance with the NERC policies.

Beyond that, we have investigations and spot audits. We've done a number of those. Some of them over the years in particular to some standards that related to control performance, as we moved into the more formal program, we now are involved with a number of other investigations including transmission loading relief investigations, we do some spot audits, and we're also auditing -- we've just recently finished auditing all of our reliability coordinators, so there's a number of activities that we're doing within this compliance enforcement program.

And I've put the last box down here as enforcement activities and we do do certainly some enforcement activities because we notify people of non-compliance and we do a number of things, but we're limited

in that, and we'll talk about that in just a minute.

What are we really going to cover today, really go into the program in a little more detail. Want to talk about the basis of the program; why do we have the NERC Compliance Enforcement program that we have. You know, why was it developed and why are we moving it forward.

The design of the program, how it's structured, how it works, the types of measures measuring methods that we use within the program. Really the status of it, where are we with it, and a little bit about where it's going, and then of course the question is the potential applicability to cyber security standards, you know, how might the program work with that, and there are, as I see it, at least a couple of options that are open, and then respond to any questions that you may have with this, I think as Alison has laid out.

The basis of the program really is simply to ensure a reliable bulk electric system throughout North America. Everything that we do in the program has a reliability basis. We're not into looking at whether or not things, someone's injured in a market or those types of activities; we're looking at it from strictly a reliability standpoint and compliance with the NERC reliability standards. And those include the operating policies and the planning standards today.

Why are we doing the program? There was a number of task forces put together in the late nineties looking at the future of NERC and how we should move forward particularly with open access and Order 888 that came from the Commission. And one of the conclusions of those groups was is that voluntary compliance with the NERC standards was no longer adequate. We needed to have a formal program and we needed to strengthen the works in our own by-laws requiring mandatory compliance to the NERC standards which was done. Our board did do that.

The next question is, okay, who does it apply to? Well really anybody's who's responsible for reliability functions. We'll talk a little bit about who that is today and who that is in the future as we move forward, that is, essentially that is changing somewhat with some of the things, and I know FERC discussed the functional model in the SMB NOPR and we'll talk about how that's going to change our program a little bit.

And of course what are we trying to do? Well it is compliance with the NERC reliability standards, and as I said, that relates to today operating policies and planning standards. We have some reliability standards in the pipeline that are essentially to take the place of those. They're to be more descriptive, have enforceable provisions in them more so than the operating policies and planning

standards that we had for many, many years.

And how do we do this? We do this through regional compliance organizations, and the programs are implemented through some regional implementation. We'll talk about that a little bit.

Today standards are mandatory on the NERC regions and their members. We do this, as I said through by-laws and the membership agreements within the regions that have requirements that the standards are mandatory throughout North America. This of course includes the U.S. Canada, and parts of Mexico.

This program was created in anticipation of enabling legislation to allow us, with FERC as a backstop, to be the self-regulating reliability arm of the industry. That legislation obviously has not happened. We're continually engaged in that process, trying to make sure that language is included in the energy bills appropriate to address that.

The program itself monitors strictly compliance with those standards and today we have no formal penalty mechanism. We have developed a, in some regions, have developed a contract-based penalty mechanism where people essentially voluntarily agree to monetary sanctions should non-compliance be identified. At least one of those regions, now called WECC the west, has filed that with the

FERC and has FERC support in that as well.

We are in the process of trying to ramp up some additional contract-based programs in the regions. They're being met with varying levels of success which we don't really need to go into today. There's just a matter of getting people to sign up voluntarily to the penalties and sanctions.

One of the things we have within our program is confidentiality of the results within the regional programs and at NERC. We do not share publicly the names of the violating entities. We do provide results of how many non-compliances, what levels of non-compliances we're finding out there, and a lot of data and information on it, but we've not been in a position where we've actually released individual companies' names as being the ones that are specifically non-compliant. We've not been asked to do that and we've held that information confidence.

The design of the program, it was really modeled after other industry-based self-regulatory organizations, primarily the securities industry and how the NAS, Mary Bender is a lady over at the National Association of Security Dealers who was on one of the task forces, a blue ribbon panel-type task forces to help us design our compliance program and the program was based around much of what's going on there where the Securities & Exchange

Commission serves as the backstop to the NASD and the NASD is the self-regulating arm of that industry.

Our program is regional based with NERC oversight. Today there are ten regional programs, one in each of our regions, that measures compliance with standards that NERC identifies to be in the program each year. Each one of the regions can monitor those participants and may, at their own discretion, include other NERC standards in that for which they've seen higher levels of non-compliance or things they believe they need to measures compliance with standards that NERC identifies to be in the program each year. Each one of the regions monitors those participants and may, at their own discretion, include other NERC standards in that for which they've seen higher levels of non-compliance, or things that they believe they need to measure specific to that region.

The primary role of NERC is to monitor the regions. We monitor the programs through audits and audit the ten regional programs and we also have some specific measures where the regions are responsible for certain standards that NERC monitors the region for compliance with those standards directly. Those are fairly rare, but we do have a little bit of that.

They said we need to talk a little bit about who must comply today, and really we're looking at entity

responsible for any part of full collector system reliability. And historically that's been defined as the control area. The control area was a concept that literally came out of, you know, the '65 black outs and you know literally as we interconnected systems, we had to come up with a way to manage the system to make sure that the system was operated reliably and the control area was developed at that time.

Fortunately today, as we move forward, we now have many more market participants with control areas were typically you know vertically integrated utilities, electric cooperatives, public power entities, etc. But today we have many more market participants with some reliability responsibility in this overall program. And to respond to that, NERC has taken a step back, and said is the control area the thing that we need going forward in the future.

In the future, we're looking to the NERC functional model. And in that model, we've identified a number of activities, functions that must take place to preserve reliability. For example, someone must balance load and generation, and we're not necessarily identifying that as a control area or an RTO or anyone else. It's just recognizing that that's a function that has to take place, and it's called the balancing authority.

There's also reliability authorities, interchange

authorities, transmission operators, several other terms that are in there. This model, for those of you who are not familiar with it, is based upon the functions to be performed. It's literally looking at what functions have to take place out there to preserve a reliable electric system. It's not based upon corporate organizations or corporate structures, and it's independent of business structures.

One of the things that we've tried to note is that as an example an RTO may serve as a balancing authority, a transmission operator, an interchange authority and even a reliability authority. Or they may just choose to not, they may not be the balancing authority; the other entities may be the balancing authority and they may pick and choose the functions that they choose to do. So that's literally why we've identified the functions and said this is not going to relate to those particular business structures that may form in the future.

What that means is we'll have to address identify what each who is performing these various functions out there and there are proposals today being circulated through our new standards process for how we certify certain entities. There's four of those entities that NERC has identified to be responsible for reliability activities and those four entities, the proposals is that they will become certified and we'll identify them through that mechanism and

they will then be responsible to comply with certain reliability standards and they'll be identify as this standard applies to balancing authorities, reliability authorities, etc.

The design of the program in the SMD NOPR we certainly noted there was some reliance and self-certification. I thought I'd talk about the assessment methods that we use today and in the NERC compliance program. They include periodic reporting. These are things that are assessed on a periodic basis; monthly, quarterly, semi-annually, etc. Generally those rely on self-reporting of data results.

A real good example of that today is our control performance measures where we're looking at how well utilities essentially mean or entities that operate generation and have responsibilities manage their control performance to maintain system frequency.

Those are reported monthly to us. There's also a standard for a disturbance if someone loses a big large generating unit. Obviously the frequency goes down and the concern is you have to be prepared for the next loss of generating resources. Those type of events are reported quarterly.

We also utilize self-certification and typically what we do in the NERC compliance program is there's a self-

certification questionnaire provided. We're asking specific questions about a particular standard and we ask for responses to that, that people self-certify that they have indeed met that standard and generally we require a fairly high level signature within the organization, typically a corporate officer's signature on many of those self-certifications.

We also have exception reporting. These are reports when an event occurs or something triggers. For example, there's a measure that talks about when you've overloaded, you've reached a critical loading operating security limit on the system, and if you've not recovered from that within a certain time frame, that's an exception and it is reported as they occur. We generally have reporting occur at least on a periodic basis so that we know for sure that in each quarter we've captured all of those and our board is looking to strengthen some of this at their next meeting.

We also have triggered investigations. These things can be triggered by a particular event on the system. Some of those are if we reach a certain level where firm point-to-point transactions are curtailed, we always trigger an investigation. As an example, they can be triggered by a disturbance or even by a complaint and there are certain investigations and audits that we will do as a response to a

complaint.

In all cases, on the first three, we follow those up with spot audits in all methods. These may be three-year periodic spot audits, anywhere from three to five-year spot checks where we literally check some of the self-certifications, the periodic reporting, look at the data to confirm that indeed what people are telling us is what they do. These generally involve site visits to operating units out there.

(Slide.)

MR. HILT: The status of the program and where we are today: We have a fully-functional program.

The program itself works well. We've identified that the process that we have identified for compliance enforcement is an effective process. We have the tools and people in place and the process itself works well.

We have seen improvements in compliance, just by virtue -- on many measures, just by virtue of being out there and measuring it. A number of entities and operating entities just really don't like to have letters of -- you know, findings of noncompliance and letters of noncompliance, discoverable in some of their files.

Our authority relies on the regional agreements. NERC has a requirement in its bylaws and the regions have requirements within their membership agreements, et cetera, that gives us the authority to have the program and to have mandatory compliance with the standards.

However, there still remains no requirement that anyone participate in a region. There's no law that says any entity out there has to be a member of one of the ten NERC regions, that I know of. And so that's simply a fact that we have good participation but we do have some situations where there are some entities who are not members of regions, and we are trying to measure compliance, and

that makes it a little difficult.

Enforcement, as I said earlier, we do have notification of noncompliance. We send letters to the companies and entities that we're measuring, noticing them that they have been found noncompliant, what the level of noncompliance is.

In all regions, there are dispute resolution mechanisms in place, if someone disagrees with the findings, so the enforcement actions are there.

The only penalties that are collected today are through and in areas and regions where contract-based enforcement agreements exist, and right now, that's only in the West, in WECC.

Within other regions, they have some more formal notification letters going to other entities, but generally we're not collecting penalties at all in the program, with the exception of the West.

(Slide.)

MR. HILT: So the final question that I had and the thing that we needed to talk about was the applicability of this to cyber security standards of our program to the cyber security standards. As I said when I sat down with Lynn and some of the other folks in our office, talking about how this might work, we really came up with two potential scenarios:

The first one was compliance with FERC cyber security standards. In this case, you know, FERC would proceed to develop the standard through the SMD NOPR or whatever vehicle that you would use, and would request NERC to monitor compliance with the cyber security standards in the NOPR or some other vehicle.

From that, we clearly would need our board approval to move forward to do that. I don't think that would be -- that certainly wouldn't be a major issue, but I think we would have to go to our board to get approval.

Looking at the schedule that we saw in the NOPR, we'd be looking at a self-certification of substantial compliance in 12 months, and it would really be 12 months after we had that approval. Self-certification of full compliance back by audits would be possible in 24 months, but we would recognize that there would need to be some auditable measures developed.

You know, standards are standards, but we also need to recognize that if we're going to do some audits and go further with this, we're going to need to know some very specific provisions as to what are we really auditing for here?

And, of course, this would apply only to FERC-jurisdictional entities, and I suppose others, through reciprocity, other vehicles that FERC may have to address

other issues or other folks.

(Slide.)

MR. HILT: In the meantime, as I understand it, the CIPAG is working through NERC, also to develop cyber security standards based upon the work that was developed with the FERC. And we are in the process of initiating an Urgent Action Standards Authorization Request to move this into -- to move these into the new NERC reliability standards arena.

That will be -- I understand that the CIPAG is working with the standards folks to do this, and they expect that shortly there will be an Urgent Action Standard Authorization Request posted for comment within the NERC circles for this.

If that moves forward and everyone agrees that we should do that, you know, the Standards Authorization Committee would bless that. There are processes developed in our agreement with -- or memorandum of understanding with NAESB that we'd also -- there's a joint committee that takes a look at these to look at the development of these standards.

And if it made it through -- certainly made it through all of those processes, then we go to the process that develops into a standard. That could be in three to six months, if this process moves fairly quickly, and it's

my understanding that it's on a fairly fast track; that those standards could be put out there.

Now, again, we would look to incorporate those; we would include them in the 2004 compliance program, and our program is an annual program. It runs from January through December every year, and we would look to include them in that 2004 program as trial use standards.

In that, what we would do, we would literally have a self-certification of compliance with spot audits on those. We would do some spot audits, primarily as a tool.

When we take a standard into a trial use, we really want to take the standard through its full test. We really want to go out and monitor this beyond self-certification, and we want to go in and do some spot audits from the standpoint of we need to learn whether or not we have this standard right, whether it's fully measurable, and then we'll come back and make some further adjustments to the standard if we don't have it.

These standards would apply to all NERC regions and their members, which, of course, includes all folks in North America.

(Slide.)

MR. HILT: Following that, a trial use standard is literally given a sunset within NERC. As I understand it, it's available for a year, while in the meantime, you

work on a -- you proceed to develop enhanced standards and a final standard from that.

We would expect from that that 15 to 18 months later, the Board will look at approving enhanced cyber security standards. Those final standards -- the standard is never final, but those enhanced standards then, with more defined compliance provisions, et cetera, would be included in the 2005 Compliance Enforcement Program, and again, we'd still -- from that we would have mandatory compliance with spot audits of the program.

As we were discussing the two potential options, both of these are currently, it looks like, almost running in parallel, and we need to -- I guess we need to determine how we're going to include these into the -- within the NERC compliance enforcement program ultimately, and if there are some other things that we want to include from the FERC as well, we need to take a look at how those might be included within the program.

And that's really all I had, Alison. I wanted to keep this fairly short and fairly high level, and I can certainly address any questions or other issues that folks may have here.

MS. SILVERSTEIN: I thought it was a very helpful explanation; thank you. Does anybody have any questions, comments, suggestions, thoughts, based on what you just

heard?

MS. McKINLEY: I'm Sarah McKinley, and I just wanted to let people know that the reason we're in this room today is not because we wanted to make this such a formal meeting, but because we had received requests from people who wanted to get a live broadcast, and we need to be in this room to get that.

And there are enough seats around this table for half the people in the audience here, and so I'm going to play Vanna White, and I'm going to encourage you to come forward. And we've got these seats around here. There is no reason why this room couldn't be used for a roundtable discussion.

That's what it's for, so please come forward, thank you.

MS. SILVERSTEIN: And I'm going to ask Kevin and Roger and Chuck to come up. And anyone named Scott is welcome to come, too.

(Laughter.)

MS. SILVERSTEIN: Mike Strange, if you all would be good enough to join us, I've got a couple of questions I think you'd be helpful on. Larry, long time, no see.

Now, the only condition is, Sarah, if you could start going around with the markers, and if you're going to talk, you have to say your name and who it is you're

representing, for our Court Reporter. Okay, good. Joe is coming down. Anybody else? Pat, do you want in on this?

It's more important that she knows who you are than I do, so take your name tag and face it toward our Reporter, if you would.

(Pause.)

The rest of you will just speak as the spirit moves you, and yell loud, right? Okay.

I want to start by posing a question while everybody is writing their name. I want to ask you the following question:

Let's go back a step and think about what is the applicability of this rule, and by that, I do not wish to get into a you have jurisdiction over us or you don't have jurisdiction over us, but rather let's go back to the functional model and how it is that an entity interacting with the grid, interacts.

And I think it would be helpful to refresh my memory. Maybe everybody else in the room knows this, but it would be helpful to me if we could go back through the discussion that you had of the NERC functional model. We've got your balancing authority, your reliability authority, interchange authority, transmission operator, purchasing or selling entity, merchant, customer aggregator, and load-serving entity.

And the question that I want to pose to you -- and I'm hoping that Kevin or Chuck and Matt and Mike -- James, I'm sorry, James, I keep seeing you sitting next to Mike in all those other meetings, and I apologize -- James and Barry, if you guys who represent particularly small utilities, can talk about which parts of the functional model, what functions your small utilities perform that you think would make them either subject to elements of the security standard or if they don't do these things, they're clearly out and it is not necessary for them to comply with that. So, do you want to start from -- maybe one of you guys, Kevin or Roger or Chuck can start with which things -- what is it that a utility, that an entity connected to the grid has to do that would make it subject to this? That is going to dictate who has to comply. So can we start with that question, please?

MR. PERRY: I'm Kevin Perry, Manager of Information Technology at Southwest Power Pool, and also the Chair of the NERC CIP Advisory Group. Alison, if I understand your question, the entities that very clearly should be subject to the securities standards would be those responsible for reliability.

Those would be the balancing authority, the people -- you know, that's the function that I most closely equate with the control area functions of today; the

reliability authority, such as Southwest Power Pool, the interchange authority, the folks that are doing scheduling between the various entities, and the transmission operator.

4

I think everybody else, the PSEs, the merchants, the customer aggregators, the load-serving entities, are more recipients of power or, you know, working in the market, and to some extent, you know, there would be some interaction on a market basis, but they are more of a user as opposed to a provider of computer services that would be responsible for reliability.

So, you know, like I said, the balancing, reliability interchange authorities, and the transmission operators, to me, would be the ones that would be applicable.

MS. SILVERSTEIN: So, if I'm a load-serving entity like East Texas Coop or something, and all I'm doing is purchasing, do I need anything besides a firewall.

MR. PERRY: Anybody who has a computer system, a computer network, needs to take appropriate security. The question that we raised when the standards were being proposed, and the intent of the standards was to deal with the security such that a compromise of an entity did not result in a cascading series of failures and compromises that would result in basically the lights going out.

If you are a load-serving entity, you've got a network, you know, you've got to define your own security perimeter, obviously, and protect yourself.

The question that has to be asked is, if somebody gets into the network of the load-serving entity, the distribution company, for example, is there a potential there for a compromise to then extend upwards, let's say, to the bulk power transmission, generation control organization? Does it have a chance of affecting that level of entity, getting up into the balancing authority, the reliability authority type of entity?

If the balancing authorities, reliability authorities, have done their job right, protecting their networks and themselves, then the probability -- you know, it's never 100-percent guaranteed, but the probability is that a compromise of the load-serving entity is probably not going to do more than just a localized, very localized impact to the reliability of the system.

MS. SILVERSTEIN: Barry and James. Have you guys been looking at some sort of screening mechanism to determine which of your members or others similarly situated small entities would have to perform the kinds of functions or interactions that would render them potentially able to harm the grid in that fashion?

MR. LAWSON: Just by way of background, on some

of our -- Barry Lawson with NRECA -- just by way of background, we have nearly two dozen GNTs, generation and transmission cooperatives that are control area operators. Those entities are members of the NERC regions where they reside.

They would be subject to the rules and policies and standards that NERC would develop through their standards development process. They're also currently subject to the operating policies and standards that NERC has now.

They perform a lot of the same functions that the investor-owned utilities perform that are control area operators, balancing, the reliability function, interchange, transmission operation.

So, those entities, it is known that they are operating a control area, and would have functions under the NERC functional model. So I don't think that there's any great mystery there.

A lot of other NRECA cooperative members are also members of the NERC regions, and they may be purely distribution cooperatives or LSEs that do not own any significant transmission or generation.

So, I think, you know, the cooperatives are integrated into this process already under the NERC umbrella, and that they will continue to do so. So I'll

leave it there for now.

MR. STRANGE: James Strange, American Public Power Association.

Our utilities are mostly -- well, we represent 1500 municipal utilities throughout the United States, and they are pretty much small utilities representing about 10,000 customers, so they are basically distribution utilities.

However, we do have some of the larger utilities that are load -- what do you call it -- control area operators and things like that.

So, in reference to your question, if I understand it correctly, these -- most of these utilities will fall under NERC and they would -- how can I put this? They would be subject to NERC guidelines and rulings in relation to cyber security. Does that answer the question?

MS. SILVERSTEIN: Yes, but --

MR. STRANGE: There's always a "but."

(Laughter.)

MS. SILVERSTEIN: You've clearly done regulation a long time?

MR. STRANGE: Surely have.

MS. SILVERSTEIN: One of the issues that we keep coming back to again and again since April when we first brought this up in the discussion of the functional model

and to whom this applies, is, how do you know if you have to comply with this or not? Merely being somebody who interacts with the grid or a member of NERC doesn't mean that this has to apply to you. It goes back to, do you have the potential to harm the grid, which is really why all of us are here and talking about this.

And I'm wondering if thought has been given to something at the NERC level or at the operator level that goes into more of a screen or checklist or diagnostic device that lets you know, okay, do I have to comply with this or not?

If this is the only way I interact and this is the only measure I have to take, if -- I'm not real worried if you're a reliability authority, because you kind of know it. If you're an interchange performer, you know that.

But if you're one of these smaller entities that has limited interaction, we're still hearing a lot of to and fro and fussing about do I have to comply and how much do I have to comply and how much is it going to cost me?

And it seems to me that the first step in a compliance discussion will have to be getting a lot crisper about articulating do I have to comply and how? Kevin?

MR. PERRY: The NERC CIP Advisory Group has not tackled this question specifically, but we have kind of danced around it quite a bit. So let me just throw

something on the table and see what kind of discussion that it generates.

Number one, if you have a computer system that is used to control the electric grid, that would be whether it's AGC, automatic generation control, pulsing generating plants such as a bulk power center would do, or a transmission distribution control center that is opening and closing breakers, you're basically using an energy management system or, at a minimum, a skater or supervisory control and data acquisition system.

Very clearly, you are doing actions, control actions that have an effect on the system. If you're doing that at the transmission level, which, you know, you can define transmission level many different ways, but whether it's 69 KV and above, 115 KV and above, 230 KV and above, you know, set your voltage level, what you consider the transmission system, if you are doing that, then those systems are the critical systems that you need to protect. At least that's a set of systems that need to be considered for protection.

We're not talking about Betty Lou's PC down in Human Resources. Now, there are other rules and regulations throughout the country that may require you to set up a secure perimeter around Betty Lou, but that's not this standard's applicability.

MS. SILVERSTEIN: Should -- we should probably avoid beating this to death by having me ask the following question: Is this a topic that the NERC CIPAG would tackle at some point so that we can get more specificity and get this issue behind us?

MR. PERRY: I believe it certainly is a topic that the CIPAG can tackle. Timeliness, you know, we can do it via conference call. Our next meeting is not until May 1st and 2nd. I get the sense that we would like to get this applicability in terms of what systems would be affected, addressed sooner than that.

MS. SILVERSTEIN: It's probably a good idea, because the next thing that affects them is how much does this cost? And there have been diverse estimates of what this would cost.

MR. LAWSON: Barry Lawson with NRECA.

Whether it's the CIPAG or whomever at NERC, I mean, as part of the standards development process, it's going to be determined, who it's applicable, so that a major part of that process.

I'm not so sure that CIPAG is the place where it will take place, where it would occur, but that is obviously something that has to be determined in a standards development process, but necessarily at the CIPAG, but in the actual process of developing the standard that Dave

talked about earlier this morning.

So I don't want to limit it to that. I don't think that -- it might not be the appropriate area to do that.

MS. SILVERSTEIN: Fair point. Thank you. But, again, to put in the marker that this needs to be -- the original intent, and, I hope, the continuing intent of this standard is to be oriented not around who does what, but what is it that is done that needs to be protected.

Let's go to Dave' presentation. He offered two options for compliance. And one of them is compliance with a FERC cyber security standard, and the other was compliance with a NERC cyber security standard, and if -- it seems to me that the distinction is at what point NERC internalizes the standard, correct?

Essentially when we closed off this topic at the last workshop, what we were essentially asking is if NERC were to do the compliance in the short term and the transition over in the long term, so I think probably we were talking about something that conceptualized starting with NERC doing a FERC standard and then the intent all along has been pretty much that NERC would own this standard and grow and change it over time. And FERC would just be a backstop; does that match other people's expectation and recollection?

MS. CONSTANTINI: Can I say something? Alison, I think that's what the intent of that option was, however, rather than use the FERC-promulgated standards to start, that it would begin with a NERC standard, compliance with a NERC standard. That's the difference.

MS. SILVERSTEIN: How much of this is doable by NERC if legislation continues to stall?

MR. HILT: Certainly, we are measuring things in the compliance program as it exists today. We are out measuring compliance, notifying people of non-compliance.

What the legislation adds is the ability with FERC as the backstop, to formalize essentially monetary penalties and sanctions with noncompliance to those standards.

So without that, certainly the standard could move forward. As Barry and James noted, you know, they're developed through a standards process that we're seeking ANSII accreditation on as being a fair, open, balanced, and inclusive process. All participants are invited to participate in the standards process.

We would envision the CIPAG as being the genesis of that, that if someone needs to develop a standard authorization request, a request to go forth and develop a standard. From that, once that's approved, then the process calls for a group of technical experts on a standard

drafting team to formalize that into a standard with the types of things, I think, that you folks are talking about here, specifically some meat on the bones, you know, specific applicability to certain areas and how do you actually go about measuring some of these things.

And so, yes, it can move forward within the context of the program, just recognizing that the limitation without legislation will be the ability at the NERC level to have real, you know, formal enforcement actions and penalties and sanctions.

MS. SILVERSTEIN: Is it possible under the current structure and lack of authority or set of agreements that exist, what sort of remedies do you have if someone is not in compliance with the standard? Isn't the object to make them compliant first?

MR. HILT: That truly is one of the goals of our compliance program is we're really not in the business to collect money. What we really want and what our real goal with the compliance program is, we want to have a reliable bulk electric system out there, and we want to ensure that people are complying with the rules to make sure that happens.

As much as we can and as much pressure as we can exert through identifying noncompliance and reporting that back to those entities that are noncompliant, certainly there's some pressure applied just by virtue of that. But that is where we are today.

MS. SILVERSTEIN: How much -- in the other kinds of work that we do here at FERC, there is a grand tradition in this industry called ratting on each other, and a lot of

what we address is because one party is aggrieved and calls to complain about the other party or throws lawyers at that in a more formal process.

Should we expect that kind of behavior, or is a lack of compliance with cyber security standards only going to show up as something that is internally discovered? And talk to me about how you know, other than a spot audit, whether somebody is compliant.

MR. HILT: Whether or not -- we have a similar rule in NERC. We call it the snitch rule. Someone's going to snitch on somebody else. And without seeing the standards or being a technical expert -- I'm not a technical expert in cyber security. I don't know whether someone passing a worm or a virus or a Trojan horse or those kinds of things to somebody else would create a situation where someone could lodge a complaint and we could then do an investigation.

The standards themselves would need to be -- not the standards, the measures themselves. There needs to be some very specific measures within some of the standards that allow auditors to go forth and take a look at an entity and say this is specific enough now that I know that you've met the intent of that, you've met the requirements of that standard.

And certainly there are a number of things. One

of the standards I think you folks had was looking at physical and electronic perimeters. There would need to be some specificity as to what do you really mean by that in terms of not only from the folks that are measuring compliance but the folks that are certainly being measured for compliance need to know what's really meant by that.

MS. SILVERSTEIN: We have a room full of technical experts, and I wonder if anyone wants to jump on that question?

MR. LAWSON: I just wanted to sort of add to what Dave is saying. For the past thirty-plus years, we've had the most reliable electric system in the world here, and we have not had legislative backing for compliance.

NRECA supports the NERC legislation that they've proposed, but it is important to keep in mind that it has worked to date through industry peer pressure and through regional, the NERC regions applying these operating policies and standards to their regions.

To do these cyber security through the NERC process is what NRECA believes is the appropriate way to do this, and not through the FERC rulemaking process. We believe that the NERC process is going to get a -- if you knew how many people were in the NERC ballot body in the standards development process that they've implemented, what is it? Is it over 300 now or 200 and some folks that? And

it's nine different segments of the industry.

It's a very large number of people that are a part of that ballot body that works on the development of standards.

We think that these standards can be done through that process and they can be enforced in the ways that NERC can do that whenever they get that charge from the industry. Right now, no, they don't have the legislative backing. They don't have the SRO sort of backing that they do for the NASD.

But we think it could still work very well the way it has worked for the last thirty years. Our members, cooperatives that are likely going to be ones that have to implement these cyber security standards, are already part of the NERC process. They're already there. You've got an organization that has the appropriate umbrella to get the right people complying with these standards. And we think that that's the right way to do it and not in a FERC NOPR/rulemaking process.

MS. SILVERSTEIN: Your objections are noted. Thank you. And I will point out that it is not the Chairman's intention to act where government should not step in where other forces are clearly handling it.

I would like to point out, however, that NERC wasn't working -- had wonderful guidelines but wasn't

approaching the standard on cyber security before FERC approached this back in April with this proposal.

So your concerns are noted, and NERC's role and important contribution in this and expertise has been long recognized and taken advantage of by the FERC in this area for the last eight months, and we appreciate that. Thank you.

MR. PERRY: Alison, to address the technical issue, you asked the question could we rat on each other? Could we know that somebody else got nailed? And the answer is, in some cases, yes.

If I set up my perimeter and I have an intrusion detection system and I'm connected to an investor-owned utility and they're compromised with a cyber attack of some sort and it starts beating on my door over my network, then I'm going to know that there's something going on.

Now the second half of that question is what am I going to do about it? Am I going to file a formal complaint with FERC? Well, that all depends. It depends on what effect it has on me. It depends on how long the incident goes on. I'm more likely going to get ahold of the investor-owned unit and say, hey, you know, I'm getting pounded on here, and you need to do something like now, and more likely work with them trying to resolve the problem, which I think in the end is what we want also.

If there is a recurring pattern of problems, then, yes, I would think at that time a complaint to FERC would be warranted. That's a decision -- or to NERC. That's a decision that would be made above my pay grade even, but I would certainly be discussing it with the executive management of my company as to whether or not a complaint would be filed.

But like I said, my first reaction is, I'm going to get ahold of my counterpart over at the company that's pounding on me and we're going to try to get this issue resolved and under control as quickly as possible.

MR. WEISS: Joel Weiss from KEMA. The only point I was going to disagree a little bit with Kevin is, we do have a number of facilities that do not have firewalls or intrusion detection. And so in those cases, it wouldn't be possible to know.

The other thing is, and this has occurred often, is that it is not always easy to try to find out where a cyber attack is coming from. And so in this case, it's very different in terms of trying to really understand where it is and, if you will, the snitching or ratting doesn't apply near as much here because it's a little bit more subtle.

MS. SILVERSTEIN: Thank you. Just to finish up on the topic of compliance, has anybody come up with a feasible alternative to having NERC handle compliance for

this?

(No response.)

MS. SILVERSTEIN: Okay. So we've pretty much exhausted the compliance area in terms of who's going to do it and what the process should be.

Roger, we haven't exhausted it?

MR. LAMPILA: Roger Lampila, New York ISO. I'd just like to go back to David's presentation. David, you mentioned that the process is through the ten regions, that there's ten region programs with the NERC corporate monitoring the regions.

My understanding is the groups within the regions are comprised of experts from the different NERC member companies that would do the work. They would do the certification work. Is that accurate?

MR. HILT: I guess I'm a little -- I'm not clear on the question. Let me try to address that.

MR. LAMPILA: Who is the member of the teams? Who makes up the composition of the members of the teams that would go out -- that go out and do compliance work today?

MR. HILT: It depends on the regions. Various regions have structured that differently. In all regions there is a regional compliance staff within the regional organization. And in general, most of the regions, they're

responsible for running the program, requesting the information, and in many cases, identifying whether making initial recommendations of compliance or noncompliance.

Often there is a peer group, as you've mentioned, that may well be part of confirming those compliance decisions. When it comes to auditing, and we've certainly done a number of those with control areas and reliability authorities, we have compliance staff and some peers on an audit team that goes forth to do that.

We do try to make sure that we have as much as we can disinterested folks involved, someone that doesn't have a material interest in the outcome of that particular audit on the teams. Does that answer your question?

MR. LAMPILA: Yes it does. Thank you very much, David, for explaining that.

I certainly can't speak positively on behalf of the New York ISO, but just knowing where we've been over the past three years, particularly as we understand the kind of information that's contained at the New York ISO as it pertains to reliability, but particularly as it pertains to the market situation, we're very, very careful who we permit through the door to look at anything.

In all due respect, I will even say that our member companies have even asked for participation in certain processes, and we've respectfully denied that, just

because of what is available, whether it's through something that's on a screen, on a piece of paper or heard through audio, once you pass the front door and come into the inner sanctum of any of the NYISO facilities.

The fact that those teams could have a composition of actually some of our market participants, I think the New York ISO may have some difficulty and may want to seek an alternative to certifying our compliance.

MR. HILT: Just a note for you, Roger, too, we recently audited the New York ISO reliability coordinator, and with all of those types of audits, we do require that the entity being audited agree with the people on the team and that they do sign, all the people on the team sign a confidentiality agreement related to that audit.

So within that light, we've gone I think as far as we can short of --

MR. LAMPILA: And I understand that. But again, reliability is important. It is the kind of information that's available on the cyber side, even looking at access rules for firewall or router. We're very, very cautious who we even show them to. We don't even permit people to have copies of that stuff. And we're very, very cautious who we even let see it.

I have made it very clear to many, many people within our organization that they're just simply not

permitted to see it. There's no need for them to see it. And life goes on.

So I know from the cyber side we're going to be very, very cautious. Thank you.

MR. NOBLE: Regarding the regions directing -- is that, if I understood what you said correctly, directing the monitoring activities, a couple of nagging concerns about that. Maybe you can explain it better so I better understand it.

One is the regions have traditionally been very heavy into reliability. I.e., the transmission and generation entities. And they do not have members from the broader market aspects that we will be trying to include in this monitoring. That's one.

And two, as you described it, I'm concerned that there might not be a necessary consistency or equity in the way the audits are conducted or the monitoring is conducted across all regions. Could you address that for me?

MR. HILT: Certainly. As I noted in the presentation, we are currently limited with regard to authority by those who are members of regions. There is no -- again, this program is a voluntary program, and if you have to have authority, you have to have a member, you have to have signed a membership agreement that includes that, without the legislative backing that is clearly an area that

we would have to address.

As far as consistency across the regions in terms of doing the audits, depending on what came out of the standards and whether there was a, as there is for reliability authorities and control areas and these other certification activities, there may well be there's a reliability authority audit procedure that is followed by everyone. There's a control area audit procedure or certification and recertification procedures that are followed by everyone.

And should those be developed, if that was a concern and we wanted to have absolute consistency, then we would need to develop a uniform procedure by which that was accomplished.

MS. SILVERSTEIN: Mr. Brooks?

MR. BROOKS: Dick Brooks. I represent CISTRENS and I also chair the Technical Electronic Implementation Subcommittee at NAESB on the retail electric quadrant. And I would just like to say that I was encouraged by Dave's reference during his presentation to the process and the cooperation between NAESB and NERC regarding this matter, cyber security.

As you know, NAESB has been involved in cyber security standards since 1996 with their electronic delivery mechanism, and very recently I had an opportunity to partake

in a case study where we implemented those NAESB standards at an ISO, and we applied the NERC security guidelines to that implementation, and we did discover some things that we think could be very beneficial to have the two organizations working together.

MS. SILVERSTEIN: Great. Thank you. Anything else for Mr. Hilt on compliance before we move to -- Roger. Sorry, I didn't see you.

MR. LAMPILA: Roger Lampila, New York ISO. I think the development of a very standard audit program has a tremendous amount of merit. I spent 12 years in IT auditing at my prior employer, and that included auditing at the New York Power Pool for ten years.

But with a very standard audit process that would be followed throughout all NERC regions, that audit process theoretically could then be used by a third party auditing firm, an entity such as New York ISO may choose to use that they would then use that to do their work.

Because of the work that is done at the New York ISO by external, you know, third-party entities, who have already become familiar with a great deal of our systems, they could actually do that work and be in and out I think much quicker than many other entities could be.

And as Kevin has indicated, I think CIPAG, continuing to help work on that, has a lot of merit. Thank

you.

MR. BROWN: Larry Brown, EEI. Dave, how is right now the NERC compliance process created? Who is involved in designing that process? Is it itself a standard, or is it something outside of the standards? If you could just explain a little of that.

MR. HILT: The program itself is outside of a standard. However, in the case of specific audit processes or procedures, those may well include, may become part of a standard that's yet to be addressed in the standards process.

There are some proposals there today for how you certify the balancing authority, and they're literally looking at certification procedures, how would we go about certifying those. Those are things that clearly NERC believes needs public vetting and through a process at the level, a full public process, such as our standards process.

And the reason I answer this, is it depends, as Roger was discussing a minute ago with some uniform audit procedures, one of the possibilities, and I think the CIPAG or those working on a standard need to recognize some of those issues as they're developing it.

And for example, I'll go back to the example where I was talking about the standard that talks about physical and electronic perimeters. It may be that the

standard just needs -- the standard that's written today says you've identified those.

Maybe the compliance provision is, you can either -- you can demonstrate through a third party that someone has signed off within the last -- I'm picking a number here -- 12 months, 24 months, and you can show us to assure that you're in compliance, you can demonstrate that through having the third party information, you know, an independent auditor essentially come in and provide that information.

MR. BROWN: So to clarify then, it is very possible that a compliance procedure, even though you've outlined what you have in existence right now, that that itself is subject to development by the appropriate community.

MR. HILT: I think so.

MS. SILVERSTEIN: So to phrase that a different way, auditing and compliance need not be one-size-fits all. You can use a different process and a different set of players to do compliance for say cyber security relative to some of the other things for which NERC has compliance, correct? Thank you, Larry.

Okay. Any other cards or hands on the general compliance topic, or shall we turn to the question of timing of compliance?

(No response.)

MS. SILVERSTEIN: Okay, timing. The original NOPR which went out ages ago proposed that this compliance begin in January 2004, but recent discussions have suggested that it be advisory in 2004 and mandatory in 2005. Anyone want to take that one on? Say yes, that's a great idea or we want it later, or bring back 2004 or any other views?

Chuck?

MR. NOBLE: Yes, that's a great idea.

MR. PERRY: I'll second Chuck's emotion. The

issue of compliance is one where we believe that the entities most significantly affected by these standards are already substantially in compliance. We also recognize that it is going to take some time for them to fully understand the issues of compliance, to identify any areas where they're maybe not fully in compliance, and to implement the appropriate remediation to do that. So there's time involved, there's budget involved. That's why the recommendation was to make it a substantial compliance in 2004 with full compliance in 2005. It gives people the chance to do that.

I think that that timing is still appropriate. I think that listening to Dave's presentation today on if the NERC compliance program is used for the compliance piece of it, with the trial compliance in 2004, full compliance with audit in 2005. I think the timing there is consistent, so I would say march on.

MS. SILVERSTEIN: And when you say "substantial compliance in 2004," is this something that is tested or do we spend 2004 and the remainder of 2003 when such standard is adopted by whomever adopts it in the process of educating each other and ourselves about what is required to make it happen and doing things like working with our friends at the Rural Utility Service to facilitate it happening effectively and quickly and cheaply.

MR. BROWN: I have a pretty strong opinion here and so I'll go ahead and jump in. I am firmly of the opinion that over 2003, we should focus our efforts on coming up with something that might be called more of a standard or at least addressing the issues of what is it by which you measure compliance with the general principles that have already been promulgated and given to FERC?

In 2004, therefore, that will probably need to be devoted to education, implementation and tweaking whatever system is created throughout this year. Frankly, I cannot imagine that in a process with a large number of people already involved, there are over 300 in the voting body now, with the addition of extra NAESB players to bring in their expertise, I just can't imagine that that will, just in developing measurable criteria and then moving on beyond that, and addressing the issue of, well how is compliance with those criteria going to be measured?

Who is going to do that, as Roger raised. You know all of those issues being a separate, essentially a separate standard, that I can't dream could be completed before at least a substantial portion of this year is over with. So I wholeheartedly agree with not shortening the time frame and just want to at least caution that it may be necessary to lengthen the time frame but I'm in no sense proposing that right now.

MS. SILVERSTEIN: Your restraint is appreciated. Scott?

MR. MIX: I agree with Larry. Scott Mix, EPRI. One of the other areas of education that I think we need to focus on is the business drivers behind being more secure. Most of the large players that we pointed out that are already substantially compliant with this have done it not because FERC or NERC or local PUCs or somebody said they had to do things, but they chose to do it because it makes good business sense.

You can save money by spending a little bit of money buying a virus protection software running on your PC because if you don't have one, you find that your PC is down for days at a time when a major virus hits. So I think the education process of getting behind why we want to have secure systems and why we wrote this to begin with, why FERC came to CIPAG and said we want you to do this, is not because FERC didn't have anything better to do and decided that they'd give a task over to somebody. It's because there are significant business reasons for doing that. And we need to spend a lot of time this calendar year stressing those business needs.

MS. SILVERSTEIN: Mr. Brooks?

MR. BROOKS: I agree with Chuck and Kevin that we do have an opportunity to reach a point in 2004 where we

have some level of security in place to support and perhaps even some form of a compliance program. I think that's possible because we do have so much infrastructure currently in place. As Scott said, a lot of folks already do implement security standards. NAESB's own EDM has within it a section entitled "Security Guidelines" that is specifically for cyber security. So if we are able to leverage some of the existing installed standards installed base, I think we do have a chance of getting to a reasonable point by January 2004.

MS. SILVERSTEIN: Anyone else want to talk about timing?

(No response.)

MS. SILVERSTEIN: Do we need to talk further about appropriate penalties and remedies for non-compliance?

MR. PERRY: Alison, I think it's a subject that needs to be addressed with the urgent action SAR and I'm kind of new to this whole process. I don't understand all the intricacies of it, and I'm hoping that Lynn will keep me honest, but my understanding is with an urgent action SAR, we are accelerating the normal NERC anti-standard process by developing the action request and the proposed standard at the same time.

But the SAR has to addressed issues of what are the measurable compliance items? What are the sanctions,

penalties for non-compliance, and the CIP Advisory Group had a conference call yesterday to launch this process. We are trying to schedule what it looks like it's going to be two-day meeting here in the next couple of weeks to try to draft this all together.

I think that it's appropriate, if FERC were to choose to use the NERC compliance process, I think it's appropriate to develop the penalties and compliance measurements as part of the existing process as opposed to trying to hash out something here.

MS. SILVERSTEIN: Scott?

MR. MIX: Scott Mix EPRI again. I think that one of the things that while we're entertaining this discussion, we need to keep in mind that the purpose of writing these standards is to be secure. It's not to go on a witch hunt and find people who aren't secure so we can crucify them.

MS. SILVERSTEIN: Hence my earlier question about isn't the first measure of compliance to make them fix it?

Having exhausted, since all of you are being so restrained, uncharacteristically, we're zooming our way through and everyone can have a really long lunch before they go back to however it is they're getting home.

Let's move to the last question which is, and I don't know how much you all have beaten this to death within the CIPAG, but in order to get it in the federal record for

this purpose, I'd like to spend a few minutes on new technical issues that weren't ripe for consideration in the CIPAG first round standard, and get some idea of what issues and challenges are on the horizon that could be showing up in NERC standard 2.0 or release 1.3 or whatever it is this thing is going to be called.

Any comments, suggestions?

MR. PERRY: Alison there are two things on the horizon which probably you should be aware of. I'm going to invite Larry Bough to speak about the PKI initiative. Larry chairs the working group under the CIPAG specific to the PKI initiative.

The second one is what I'm calling ICCP or inter control center communications protocol security. IEC Technical Committee 57 working group 15 met about a year ago, and identified a proposal and had EPRI sponsorship, identified a proposal to introduce a certificate security for the purposes of and authentication and encryption of the real time data which includes not only telemetry being reported but also the capability to issue control actions via the ICCP protocol.

That process has continued to march forward. Working Group 15 deals with security issues and that is basically headed by a gentleman named Herb Faulk of SISCO, S-I-S-C-O, the folks that make the underlying communications

handler, something called MMS.

Brent Brobach of ESCA also MESCA Corporation heads up Working Group 7 which has the standards for ICCP in the first place, and the two of those groups have been working very closely together. Within the past couple of weeks, ESCA has gone out to their user community once again, identifying that they are implementing the security standards that were proposed within their implementation of ICCP.

SISCO is going to be developing for the MMS product, is going to be developing the actual digital certificate handling and interfacing. I understand that there's another EMS vendor that is also signed on to participate and incorporate it into their product. So basically a very large percentage of the installed ICCP users within U.S. and Canada will have, within the next four to six months, will have availability of this particular capability.

Unfortunately, to make it mandatory across all of ICCP requires action by the International Standards Body to incorporate it as an actual part of the standard. There's standards body covering MMS. There's the different standard body covering the ICCP or TASC.2 standard that ICCP is governed by. But I would encourage FERC, NERC, everybody who uses ICCP, to participate in this to start using it. I

think it's a major step forward in securing the intercontrol center data exchange which is a very key part of our reliability operations.

I said I'm going to let Larry discuss the PKI initiative which is the other one that I had on my mind.

MS. SILVERSTEIN: Let's let Larry go first, please.

MR. MIX: ICCP follow on.

MS. SILVERSTEIN: Okay. We'll get back to you, Larry.

MR. MIX: Yeah, we're not going to forget you, Larry. There's some further work being done by EPRI this year in ICCP specifically performance and our operability testing. We need to make sure that the proposal that was written in spec form and white paper form at the end of last year is actually practical. So there's a lot of work being done in that.

The other thing is that one of the facets of the proposed design is seamless interoperability between running the new encrypted version of ICCP and a non-encrypted I'll call it traditional version of ICCP simultaneously so that if you are running in a large participant network, and not everyone is moving towards the new version at the same time, or is capable, due to budget or resource or version constraints, maybe some people can't move to the new version

in a timely manner. That the two versions can operate simultaneously.

MR. WEISS: Joe Weiss, KEMA. For what it's worth, I was the EPRI project manager several years ago doing the ICCP demonstration projects between control centers and power plants. I also happen to be on the IECTC-57 Working Group. The concern that I have out there -- and I was also the one who brought forth the EPRI efforts and the need to address ICCP -- the concerns are that part of ICCP does is it has a block to do control.

MS. SILVERSTEIN: We're not going to argue now, but whether it's good work.

MR. WEISS: No, I'm just concerned simply that the control systems themselves are not being addressed by that, and that's the concern I have because within the perimeter that's being addressed within the NERC rule, is the ICCP server. And that's why I have that concern and that's the only reason I'm bringing that up.

MS. SILVERSTEIN: Larry?

MR. BOUGH: I'm Larry Bough from ECAR. I'm vice chair of the CIPAG and as Kevin said the group that's spearheading the NERC PKI effort. PKI is Public Key Infrastructure and it deals with the use of certificates or some mechanism to authenticate users and to encrypt and de-crypt data transfers so that we secure the information. We

also can ensure that the information is being exchanged between two folks, two parties, two machines, whatever, that really know that yes, I'm Larry Bough and I'm talking to Alison Silverstein, and she's talking back to me kind of thing.

We were requested, the CIP AG was requested by the NERC Electronic Scheduling Collaborative, an OASIS standards collaborative about year, year-and-a-half ago to implement a PKI based on a certificate policy that they had delivered to us at that time, the EMARC certificate policy. We've been working on that for some time, put together a self-directed work team within the CIPAG to address it, to look over the certificate policy and ensure that we wanted to take it to the NERC Board for implementation.

We did agree that, yes, it needs to be implemented. We took it to the board last February. They approved the project and since that time we've been working on trying to bring that project to fruition. Right now we've got a schedule date of this September to bring PKI up when in fact we have a meeting of the work team tomorrow here in D.C. to continue developing are implementation.

What we intend to do with it is to secure -- we've identified a list of applications that are industry applications -- OASIS, tagging, those sorts of things that are already out there, and in some cases already use PKI or

some mechanism to secure the data transfer. Those would be the primary candidates for a pilot project to make sure that our program is working the way we want it to.

And then what I would anticipate is in answer to your question originally is with PKI, that would be one of the technologies that I think a version 2 of the NERC standards would in fact reference, and suggest that as a standard, the PKI implementation, EMARC implementation be the standard for securing data communications for a list of data exchanges, both market and reliability-related data could and should be secured using that kind of an implementation.

MS. SILVERSTEIN: Thank you. Mr. Brooks?

MR. BROOKS: Dick Brooks representing NAESB. The concern I have regarding PKI is that there is an installed base today within NAESB using self-signed certificates, and these entities aren't required to go through any type of formal registration authority or certificate authority, and was just wondering if you do plan to allow self-signed certificates?

MR. BOUGH: Within the PKI implementation that we're looking at would apply to industry-wide applications and in fact I should have mentioned that we do in fact have a representative from NAESB on the work team who's working with us. We have folks from AGA, APA, who are also working

with us to make sure that we do in fact come up with an implementation that if we want to spread that implementation outside of the electricity industry itself to other related industries or co-supporting industries, if we've got a gas and electricity entity out there, then they can use the implementation.

In answer to your question, those applications that would be secured using EMARC would be only secured using certificates that come from EMARC compliance certificate authorities. If you have back end applications that you want to continue using self-signed certificates to use for those, then you're certainly welcome to.

The other thing that we intend to do is to provide a transition period. We know that we can't just ask everybody to switch to an EMARC certificate on such-and-such a day; that's not going to work. So one of the things that we're wrestling with is how do we put together a transition period that allows folks who do have certificates but need to eventually transition to an EMARC certificate to make that transition.

So in answer to your question, no, the program does not ultimately allow for self-signed certificates; they will be certificates issued by a EMARC compliance certificate authority. And only those certificates would be allowed for those applications that we identify through the

standards process of needing to be secured with EMARC.

Does that answer your question?

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

MR. BROOKS: Yes, thank you.

MR. PERRY: One of the benefits of introducing the EMARC standard for things like OASIS, tagging, and scheduling, is that it then forms the root around which other entities are probably going to start using the same certificate. There's a lot of market force drives out there, market participants who would like to have one certificate for web-based activities, which says, hi, my name is Kevin Perry; I work for Southwest Power Pool, and I'm a good guy.

And that's doesn't mean I have permission to get into your system, but here's my credentials. And if we make it a requirement that applications that are used NERC-wide, such as OASIS, you know, will accept these certificates, then Kevin Perry, subject to each OASIS node administrator granting me an actual permission to get into the system, Kevin Perry can use his one certificate to go wherever he needs to go to do whatever he needs to do, without having constantly having to close the browser out, starting it up again, so I can select yet today's certificate for this action.

Now, you can then extend that to non-NERC applications, if you will, such as market operations systems where I'm a market participant and I am trying to use, let's say, the PJM or the MISO market system to do my business.

If I can use the very same certificate, once again, subject to them allowing me into the system, the trust model of the EMARC certificate is that we're trying to design it in such a way that the entity can rely upon the fact that I have this certificate, that I have been properly vetted; that I have identified who I am, you know, properly; that I have the proper rights to want to do this business.

That doesn't mean that they throw away all of their security. It doesn't mean they throw away all of their procedures.

What it does do is it enables a somewhat more seamless interaction between the various service providers and the customers of those services. So, hopefully, you know, as this comes along the, groundswell will spread this out beyond just the NERC standard applications.

MS. SILVERSTEIN: Thank you. We have ICCP; we have PKI. Are there any other letters of the alphabet that represent new technologies that we should be looking at on the horizon? Dick?

MR. BROOKS: Yes, Alison. NAESB has used PGP since 1996. And PGP is a similar model to PKI, only it depends on a different trust model; it depends on a web of trust where individuals use -- companies use trading partner agreements to enforce their trust models and the legal aspects associated with them.

So, I would encourage that this group, this PKI group, consider some form of a backwards compatibility with PGP in order to bring in that installed base that exists in the current market.

MS. SILVERSTEIN: And I'm afraid we'll have to insist that you spell out PGP, in case it's not what I think it is.

MR. BROOKS: Okay, it's pretty good privacy.

(Laughter.)

MR. BROOKS: There's actually -- it's a newer model now. It's a standard in the ITEF called open PGP.

MS. SILVERSTEIN: I was hoping it was going to be really good privacy.

(Laughter.)

MS. SILVERSTEIN: Anything else in terms of other technologies?

MR. SORENSON: I'm Paul Sorenson. I'm representing OATI today, but I just wanted to let everyone also know about the work of the OASIS Standard Collaborative. That has been trying to look at OASIS, Phase II, as a result of the advanced NOPR, which was then supplanted by the SMD NOPR.

But in April of 2001, and reconfirmed in the Fall of last year, that identified foundation technologies that they felt were going to be part of OASIS, Phase II. And I

know this isn't -- the NOPR doesn't address the technical communication protocols and standards, but we know they will come, they will come through a NAESB process, but we have already said, you know, subsequent to review and change, we were going to promote PKI, secure sockets layer, which uses that, and a web services type of technology model in terms of data exchange.

So, one more acronym for you, web services, which you can then rattle out. But there are other things that I think will come out through the NAESB process of communication standards.

MS. SILVERSTEIN: Good, because I was worried. Okay, Mr. Charmal?

MR. CHARMAL: I'm Matt Charmal, NRC. We have a new -- we're finding out that they're using wireless data communications coming up pretty soon, and that's one of the areas that we will be looking into.

MS. SILVERSTEIN: With respect to improving the security of the wireless communications?

MR. CHARMAL: Yes.

MS. SILVERSTEIN: Okay, thank you. Joe?

MR. WEISS: It's longer term, but there is technology now being developed for securing control systems. We have not in any way, shape, or form, addressed that, but in the longer term, I think we're probably going to want to

say to some extent, to use available best technology. It's just not there yet, so, therefore, it's not been applied.

MS. SILVERSTEIN: Thank you. We have run through the topics that were on my list of things that needed to be addressed that were cleanup items or followup from the prior technical conference, and it looked as though they needed to be discussed and thought about for us to move ahead on implementation and compliance issues for cyber security under SMD.

Have we left out any issues, any questions, any closing thoughts that people feel the need to share? Chuck?

12

MR. NOBLE: Yes, thank you, Alison. You're bringing this to a close, and I have a couple of thoughts I'd like to share, and maybe come back full circle.

You started off with the question of if someone was only involved in the market, would they only be required to have a firewall? And I'd like to sort of reposition that question and look at it in terms of what's the real minimum that we would expect to see across the board for everyone?

And I think that would start with pretty much the way we presented the items in the standards themselves, and that starts with governance.

At a minimum, I would expect to see everybody have identified that senior manager, or, in a larger

organization, an actual officer of the company, to be responsible for their security program, okay? Or, to be specific, their cyber security program, but it could be their security program overall. I don't want to limit that.

The second thing is to begin to develop their strategies and their policies. Okay, these are things that can be low-cost and there should be no impediment to them having these place by January of 2004.

These are the kinds of things I would look to see as minimums, okay? Also, around the issue of personnel issues, having established the programs around training, employee awareness, and policies and practices, et cetera, I'd like to see that on the table as the minimum, that, regardless of who you are, what your organization does, how it does it, how it's configured, this is what I expect to see from everybody.

Whether or not they would actually have a firewall or some other solution isn't quite the question from that perspective.

The other thing too is I also want to take the opportunity to encourage people, particularly the IT people, the cyber security people, to really partner with the other side of the security house, the physical security people, or the operations people, okay. Because I think many people will find that not all of the solutions need to be technical, okay.

So they really need to partner and make it a team across the board. And with that, I thank you.

MS. SILVERSTEIN: Yes sir?

MR. BROOKS: Alison, just one more comment. We talked today quite a bit about ICCP and PKI and PGP, but the reality is, many of the companies, organizations that are out there working in our industry are also subject to other risks.

We didn't talk about, for example, securing Web servers. A lot of corporations, the utilities and other organizations in our industry, run these Web servers, and many of their networks are connected in some form or fashion to yours or mine or their own internal networks.

And so there are some initiatives underway at NIST under the SP800 series of documents that we should also

consider as well.

MS. SILVERSTEIN: Thank you. Those are absolutely correct points and probably the reason we didn't bring them up earlier is because we have been trying to keep focused very cleanly on, gee, if you lose your systems, too bad for you, but we're focused very cleanly on what systems are needed to protect grid operations and market operations.

You're absolutely correct, though, that those systems are critical to a business functioning and should be protected in a cyber fashion. So thank you for bringing that up.

MR. BROOKS: It could in fact be connected to the very systems we're talking about trying to protect.

MS. SILVERSTEIN: Right. Scott?

MR. MIX: That actually supports my point about the business justification for being secure. One of the things that -- the outcome of this should be that a company of substantial size should have a single set of consistent security practices so that their Web servers and mail servers, for example, are at least as secure as their control servers and their market servers.

MS. SILVERSTEIN: And remember that we are talking minimum daily adult requirements to protect the grid and not the other things that a company with any self-respect should be doing on its own to protect its IT

systems.

MR. MIX: From a FERC regulation and NERC regulation standpoint, but not necessarily from an internalized company policy standpoint.

MS. SILVERSTEIN: Yes, Kevin?

MR. PERRY: I would just like to offer a couple of thoughts. Number one, I think what Scott is saying is extremely important. Security -- we have focused on minimums standards. We have focused on critical systems, but woe be to the company that says, well, I don't need to protect this network or I don't need to protect this system because FERC didn't tell me to do so and NERC didn't tell me to do so.

All of our systems and all of our networks are very tightly integrated with each other, and if you have a disruption on a noncritical network that because of the interaction and interconnection impedes your ability to conduct business over your critical network, then you've got problems.

A lot of decisions that are made today by companies are made based on cost. It's very, very inexpensive to put in a Windows, Microsoft Windows-based platform as opposed to a UNIX-based platform. That doesn't mean that you cannot secure Windows. You certainly can. There is a lot more opportunity to be attacked with Windows

because it's there and it's so widely used, not that it's any more or less secure than anything else. I don't want to get into Microsoft bashing by any means.

But the issue is that decisions are made based on cost. And it's cheaper to do a VPN tunnel over the Internet to communicate between two sites than it is to put in a private frame relay network, and that works incredibly well until you have an event like a weekend ago where the SQL slammer, also known as Sapphire, worm came out, and there was so much traffic on the Internet that you couldn't get a word in edgewise.

If you look at some of the casualties. Bank of America's ATM system was severely impacted. Wells Fargo's was not. I believe it was Continental Airlines had to cancel flights out of Houston because of impact to their systems.

There was a tremendous amount of damage and impact caused by this rapidly growing, rapidly spreading worm, which is very likely to happen again. If you've made a decision based on cost to route your traffic over the Internet and you have no Plan B, then it doesn't matter how well you protect your critical cyber systems. It doesn't matter how good of a lock you have on that room door, you know. You have not taken a holistic view of the whole thing.

Yes, that's more into the best practices than the minimum daily standards. The problem is that we find out after the fact, we react rather than proact. And when we let dollars be the sole decisionmaking process for how we secure our systems, we're really looking at the wrong thing. We really need to understand business impact of that decision if something goes wrong.

MS. SILVERSTEIN: You've made a good case for the public interest in asserting cyber security. And on that note, I will declare victory and thank you all for coming today.

(Whereupon, at 11:22 a.m. on Tuesday, February 4, 2003, the Cyber Security Conference was adjourned.)